

**APPLICATION FOR  
UNITED STATES PATENT**

**in the name of**

**Clayton Kittrell, Benjamin Wright, and Ray Grubbs**

**For**

**TRANSPORTABLE DOCUMENT IDENTIFIER**

Express Mail Label Number: ED901607264US

**ATTORNEY DOCKET:**

**03.B.002US**

# TRANSPORTABLE DOCUMENT IDENTIFIER

## CROSS REFERENCE TO RELATED APPLICATION

This application claims priority to U.S. Provisional Application No. 60/412,353 filed September 21, 2002, is a continuation-in-part of U.S. Application Serial No. 10/214,444 filed August 8, 2002, and is a continuation-in-part of U.S. Application Serial No. 10/367,964 filed 5 February 19, 2003, each of which is hereby incorporated by reference in its entirety for all purposes.

## TECHNICAL FIELD

This disclosure is directed to the use of an electronic signature or as a memorial of certain facts where some or all of the facts are not electronically available.

10

## BACKGROUND

Every day significant business transactions take place electronically. The Census Bureau of the U.S. Department of Commerce estimates that electronic commerce sales in the United States totaled \$9.849 billion during the first quarter of 2002. Typically, transactions are conducted by users selecting desired products or services through a website. The user 15 then provides payment information, such as a credit card number, and acknowledges the transaction by clicking on a button. These transactions may be conducted without requiring physical or electronic signatures.

In 2000, the U.S. enacted electronic signature legislation designed to afford electronic signatures the same legal weight as written signatures. This law allows many transactions 20 required to be in writing to be executed electronically. Despite legal acceptance, it is uncommon to enter into some transactions, such as insurance agreements or real property transactions, using anything other than a written signature.

Much of electronic commerce occurs across the Internet, where consumers have instant access to a plethora of information. Consumers may use an increasing variety of 25 devices to conduct electronic commerce across the Internet such as, for example, computers, mobile phones, and personal digital assistants. For example, using a wireless access protocol (WAP) enabled mobile phone, a user may browse and purchase products for delivery.

While even expensive products may be purchased electronically, some transactions usually are not entered electronically. For example, a consumer desiring an insurance policy for a car, house, or boat may be able to apply for an insurance policy electronically; however, most insurance companies require that submitted information be confirmed and signed in writing before issuing the policy. Some insurance companies may issue temporary binders that terminate in a short period of time unless a signed, written agreement is timely submitted by a customer.

Similarly, real estate transactions are rarely carried out electronically, though a home buyer may identify the house of their dreams through a website, contact the listing real estate agent via email, and apply electronically for a mortgage. Despite the home buyer's reliance on the Internet through the whole process, the transaction closing typically involves the home buyer signing a stack of papers before a notary public.

## SUMMARY

In one general aspect, a method for facilitating voice signatures includes identifying a document to be signed, creating a speakable identifier summarizing the contents of the document, creating a voice script including the speakable identifier, and using the voice script and the document to be signed to facilitate the creation of a voice signature.

Identifying a document to be signed may include identifying an electronic record containing one or more details of a transaction and/or identifying an electronic record containing a document to be acknowledged. In some implementations, creating a speakable identifier summarizing the contents of the document includes calculating a cryptographic hash, checksum, and/or message digest of the document

In some implementations, using the voice script and the document to be signed to facilitate the creation of a voice signature includes creating instructions using the voice script such that the instructions enable a signer to create a voice signature. These instructions may be forwarded electronically or in hard copy to a signer for execution.

In another general aspect, a method for creating a voice signature of a document includes receiving instructions including a voice script and an indication of a document to be signed, the voice script including a speakable identifier summarizing the contents of the document, recording a user reading the voice script, and creating a voice signature including

the recorded reading of the voice script. The instructions may or may not be included with the document to be signed. The document to be signed may be received in any format, such as, for example, electronic format or hardcopy.

5 The details of one or more implementations are set forth in the accompanying drawings and the description below. Other features and advantages will be apparent from the description and drawings, and from the claims.

### DESCRIPTION OF DRAWINGS

FIG. 1 is an exemplary network architecture for creating an electronic signature corresponding to data.

10 FIG. 2 is a flowchart of a method for creating an electronic signature corresponding to data.

FIG. 3 is a diagram of document execution and verification in an electronic signature system.

15 FIG. 4 is a diagram of web-based document execution in an electronic signature system.

### DETAILED DESCRIPTION

In conducting transactions, one may be asked to sign a document such as, for example, a check, an agreement, or an application form, typically by affixing a written signature to the document. A signature is a symbol adopted with the intent to authenticate a record or document. There are no magical incantations required; it makes no difference whether a signer signs his name, places an arbitrary mark (e.g., an "X"), or draws a picture. The efficacy of the signature rests in the intent of the signer's action.

20 Some systems provide electronic signature capabilities using digital certificates relying on public-key cryptography. In such a system, users are issued electronic credentials containing public keys, with each credential being associated with a corresponding private key. A user is presented an electronic document and given the ability to sign the electronic document using cryptographic techniques by applying his or her private key to a hash of the document being signed to create a signature for the document. The user's credentials and the signature are associated with the electronic document and can be used to verify that the user signed the document.

5 In other systems, a voice record may be created and associated with a document. A voice record is an audio recording that may be used as a memorial of certain facts or as a signature, expressing an intent to affirm a record or transaction for legal purposes. When used as a signature, a voice record may be referred to as a voice signature. As with other types of signatures, the litmus test with voice is the ability to show that a "voice signature" was adopted with the intent to authenticate a record.

10 Increasingly, electronic devices (e.g., computers and personal digital assistants) are capable of recording voice statements. Analog devices such as tape recorders are also capable of recording voice statements. These devices may be used to record an individual's voice to create a voice record showing that a particular person stated particular words. These words may indicate the facts memorialized by the voice record, or may indicate a reference to a certain document or facts.

15 In these and other electronic signature systems, the emphasis is on the input, capture, and securing of a particular symbol intended by the signatory as a signature. For example, an electronic signature system may capture a record, token, code, number, key, voice recording and/or biometric recording.

20 Under the Uniform Electronic Transaction Act and the Electronic Signatures in Global and National Commerce Act, "electronic signature" has been broadly defined. The implementations described below take advantage of this broad definition, using a process as an electronic signature. In these implementations, an electronic signature is not merely a symbol; rather it is a process initiated by a signer of a document to indicate the signer's intent.

25 Referring to FIG. 1, an electronic signature system 100 includes a workstation 102 that accesses a server 104 across a network 106. The workstation 102 is an electronic device, such as, for example, a computer, a personal digital assistant, a cellular phone, a video recorder, or an audio recorder, capable of creating an audio recording for use in a voice record. The server 104 is a computer server capable of facilitating the signature of a document or facts using workstation 102. An electronic signature, described in detail below, captures a symbol that contributes to showing intent, but the symbol itself may not be sufficient to show intent. An electronic signature executes a process which in its totality is indicative of the signer's intent to sign the document or transaction in question. The

workstation 102 and server 104 communicate across a network 106 which may be implemented using any communication technique such as, a direct cable connection, a local area network such as Ethernet, or a wide-area network such as the Internet. The process signature system 100 may execute a process constituting an electronic signature as described below.

5            Electronic signatures typically are applied to electronic data. In a conventional electronic signature system, a document is presented to a signer for the review and execution. However, a signature still may be captured even if the document is unavailable or partially available electronically. Using the electronic signature system 100, a signer may execute a 10          document even if the system 100 does not have immediate access to the entire document in electronic form using a signature process that includes capturing a voice statement made by the signer to infer his intent to sign the document.

10           Referring to FIG. 2, a signature process may be performed by receiving an indication of information to be signed (step 202), such as, for example, a reference to a document 204 to be signed. The document 204 identifies the information to be signed. This information may be kept in any form and may include portions or may be entirely in a non-electronic format. For example, the document 204 may be a paper contract that is mailed or otherwise delivered to the signer. The document 204 may include any information, such as, for example, details of a transaction, a contract, terms of an agreement, an electronic message, and/or the contents 20          of a file.

20           The electronic signature system 100 then engages the signer in a signatory process by instructing the signer to perform some action (step 206). For example, the system may display a message to the user indicating that the user is engaged in a signatory process and that at least some portions of the process will be recorded as a memorial of the signer's participation in the signatory process. Once the signer has performed an action, the 25          electronic signature system 100 receives signatory information from the signer (step 208).

30           The electronic signature system 100 does not present the document 204 for the signer to view at the time that he executes the signing process—the circumstances of the signatory process may assure the signer that his voice is being associated with the document 204 that he intends to sign. For example, the system 100 may inform the signer that the document 204 was presented to him in printed form. Alternatively, this system 100 may be used when

the signer trusts a person (such as, for example, an attorney or agent) who has reviewed the document 204 or otherwise overseen the process.

The system 100 optionally may continue instructing the signer (step 206) and receiving signatory information (step 208). This signatory information may come from any action taken by the signer including, for example, a mouse-click, a typed phrase, a voice recording, or a biometric reading. Finally, the system 100 creates a process record 210 (step 212) including the electronic document 204 and information describing the signatory process used by the signer. In addition, the process record 210 may include records of actions taken by the signer.

The signatory information includes a natural expression of acceptance, which is a recordable human act that expresses some reference to the electronic document 204 being signed and that others perceive as a reasonable display of intent. A natural expression of acceptance may include a voice statement, a series of gestures, a series of handwritten statements, other human expressions, or any combination thereof.

For example, one implementation of the process signature system 100 builds on the voice signature system described in U.S. Application Serial No. 10/214,444 titled "Voice Record Integrator" and filed August 8, 2002 (the '444 application). In this implementation, workstation 102 displays an image of a document being signed and instructs the signer to initiate a process to sign the document. The process includes generating a document indicator that summarizes the content of an electronic document 204. The document indicator is used to form instructions to the signer directing that he speak a script with his voice (step 206). The signer follows the instructions and the oral statement is recorded (step 208). The recorded oral statement is stored along with an explanation of the signature process (step 212) to create a process record 210.

The document identifier summarizes the contents of the document into a form that is easy for the signer to manage, thus contributing to the circumstances of the signatory process, giving the signer (and others) some confidence that the signer executed the intended document using the signatory process. A document identifier may be selected such that it may be easily read (or remembered). The signer speaks the document identifier so that his voice statement is linked to the document in question. The document identifier deters mistake and fraud by referencing the content of the document 204.

This system 100 enables a document to be signed when it is not economical or convenient to display or vocalize the content of the document in electronic format.

If the process record 210 includes a sufficient description of the signature process such that one may later verify the process record 210 is a valid electronic signature, then the 5 record is said to be self-explanatory. A process record 210 is transparent if it is self-explanatory and contains or refers to all information (including technical information) necessary for an investigator, years after creation of the process record 210, to analyze the authenticity of the document 204 and the accompanying natural expression of acceptance. A transparent process record 210 does not rely upon secret information, does not refer to 10 external material that is not widely available, and does not rely upon file formats that are not widely supported. For example, a transparent process record 210 should not assume that an investigator will be able to retrieve secret documentation, algorithms, keys, codes, or devices from anyone, including the developer of the software that created the process record 210.

An electronic signature that is created using secret information may be difficult to 15 later verify and may only be verifiable by one party. For example, suppose Bob and Alice create an electronic signature for a document using a process that requires secret information known only to Bob. Suppose further that Bob and Alice each posses a copy of the electronic signature. If a dispute occurs over the authenticity of the electronic signature, Alice would be at a great disadvantage because Bob controls the secret information needed to verify the 20 signature. Additionally, if processes and signature systems are changed over the years, Bob may no longer have access to the secret information needed to verify the signature. If Bob and Alice had, instead, used a transparent process record 210, then each would be able to properly verify the signatures using the included description of the signature process.

A natural expression process, combined with a self-explanatory record, yields a 25 signature approach that is more informative to a future investigator than are traditional electronic signature approaches. For example, a document electronically signed using only conventional public-key cryptography only permits verification that the user (or someone with access to the user's private key) initiated a process to sign the document. This signature does not indicate the signer's emotions or state of mind. But a natural expression process 30 allows the signer to express his sense of understanding, deliberation, free-will, acceptance, closure, and commitment with respect to the document. This greater range of expressiveness

deters ambiguity and mistake when a future investigator, relying on a self-explanatory record, interprets the significance of a signature. Further, this greater range of expressiveness promotes transparency in the final record because it can reliably convey the signer's intent without the use of secrets.

5        A process-based signature carries practical implications that are different than those for a symbol-based signature. For example, if a signature is an expressive process that includes capture of a voice record, a flaw in the recording of the voice does not necessarily invalidate the signature. The fact that the signer tried to execute the process could be a sufficient expression of intent to effect a valid signature. But if the signature is a voice record alone (i.e., a symbol), then a failure in the process for capturing the voice record prevents a valid signature from occurring.

10

15        Many electronic signature systems rely on computational security to verify a signature using, for example, cryptography or encryption techniques to store data with a signature to ensure that the signature and the document to which it is linked are not tampered with or modified. Computational security implies the use of some secret key, code, method, device, record, or algorithm. Without the secret, anyone could change the components inconspicuously. A secret action that cannot be reproduced at some later time by an investigator renders the final archive non-transparent. The techniques described herein may be used independently of any computational security techniques by basing verifiability on a recording of a natural human expression, incorporating indications of intent (and/or deliberation) into the same data entity that shows a link to the document content.

20

25        For example, a process signature may include a recording of John's voice as a natural human expression of intent, vocalizing a speakable document identifier. An investigator may analyze the recording to hear what purports to be John's voice. The investigator may then evaluate the way in which the voice in the recording sounds. Using this analysis, the investigator may determine whether it is in fact John's voice and whether the signature is valid based on whether the recording conveys John's understanding, deliberation, free-will, acceptance, closure, and commitment with respect to the document. The investigator may determine that the recording is John's voice and John had the requisite intent; that the recording is John's voice, but John did not have any intent to accept the terms of the agreement; or that the recording is not John's voice. In this implementation, the

30

investigator's evaluation of John's voice is indistinguishable from his evaluation of whether John's voice links to and speaks a document identifier for the document in question. The voice record, the forensic information conveyed by the voice, and the information that links it to the document are entwined as a single data entity. In other systems, an investigator may analyze various gestures or other natural expressions in addition to voice recordings to verify a process signature.

5 While computational security may be more cost-effective, signatory processes incorporating natural human expressions may be more effective in convincing human decision makers, such as jurors in a courtroom.

10 The '444 application describes the use of a speakable identifier to record a voice signature. A speakable identifier is a code that is easy to vocalize. A speakable identifier enables the recording of a voice statement of intent to be reliably linked to a particular document. Repetition of a speakable identifier within, for example, a voice statement promotes transparency in a final signature record because it reliably links the signer's 15 statement of intent with the signed document in a way that avoids secrets. Repetition of a speakable identifier within any natural human expression of intent promotes transparency in the final record.

20 In the '444 application, the speakable identifier includes some representation of the document being signed, such as, for example, an MD5 hash of the document. Many different speakable identifiers may be used in this system. For example, the speakable identifier may be a document reference number, a hash of part of the electronic document 204, or a digest of the document created through some algorithmic process. In these systems, the voice record or archive may be supplemented with a record that describes the signature process, so as to facilitate future authentication and analysis of the electronic signature.

25 For example, in some implementations, a voice record uses a digest of key parts of a document and not a digest of the document itself as a speakable identifier. The key parts may, for example, be all of the visible alphanumeric characters in the document, arranged as they would appear in the document, but omitting spaces, formatting, punctuation, graphics, and non-visible material. A checksum or hash taken of these key parts almost certainly will 30 be different than a checksum or hash taken of the entire document. An investigator verifying an electronic signature would not be able to verify that a recorded oral statement included the

appropriate document identifier unless the investigator discerned the appropriate process used. If a process record 210 is created containing all of the information contained in a voice record as well as a description of the process used to create the voice record, then the resulting process record is much easier for an investigator to later analyze.

5 If the document 204 is unavailable electronically or partially-available electronically, a user may enter sufficient electronic information into the system create a speakable identifier.

10 The system 100 may describe the signature process in a process record 210 in any manner such that the process used to create the record may later be discerned. If the signature process may be sufficiently discerned from a process record 210 alone, then the process record 210 is transparent. The process record 210 may include a description of the signature process in any manner. For example, the signature process may be described in a textual record that is included in the process record 210 and identifies the specific process used to create the electronic signature. The textual record may include information such as, 15 for example, identification of the letters and document components used to create a hash, a description of the hash algorithm, and/or step-by-step results of the hashing process.

20 Referring to FIG. 3, a process signature system 100 may be used on a terminal 302 to execute a document 304. The signature process 306 creates a signed document 308 that is stored as a process record 210 including at least the document 304, a description of the signature process 306, and a natural expression of assent.

25 In a specific implementation, John Smith, an employee of a state welfare agency, prepares an electronic record of a welfare benefit form to be signed by a citizen, Jane Doe. The form is prepared on a terminal 302 that is a Dell personal computer with a Pentium III processor and 128 megabytes of RAM, running the Microsoft Windows XP operating system and the Microsoft Word XP application. Smith prints the form onto a sheet of paper with a Hewlett Packard laser printer attached to the terminal. This form is the document 304 used by a signature process 306 to create a signed document record 308. Jane Doe desires to sign the form so that she may receive welfare benefits (step 310).

30 To allow Jane Doe to sign the letter, John launches a software program that facilitates the integration of a signature process with the letter (the "signature program") (step 312). The signature program runs a cryptographic hashing algorithm against the visible

alphanumeric characters in the letter's content (excluding spaces and formatting), which results in an alphanumeric digest identifying the document (similar to that described in the '444 application). To make the alphanumeric digest easier for users to pronounce and use, it may be summarized or shortened using techniques described in the '444 algorithm. In this 5 example, the summarized digest happens to be "ABCDE." The signature program prepares instructions for Jane Doe as to how to carryout the signature process (step 314). The instructions state that Jane Doe may sign the form by calling a telephone number, indicating that she wishes to sign a particular document (e.g., welfare benefit form 1234), and speaking the following script: "I, Jane Doe, hereby sign my July 2002 welfare benefit form. The 10 signature code is ABCDE."

The signature program enables John Smith to print the instructions using the printer. The instructions and welfare benefit form may be mailed to Jane Doe so that she may execute the form using the included instructions. The electronic welfare benefit form is stored in electronic form (e.g., as a Microsoft Word document).

15 When Jane Doe receives the instructions and the welfare benefit form, she can sign the document by following the instructions. Jane Doe dials the identified telephone number and enters an interactive voice response (IVR) system. She indicates, by pressing numbers on her telephone or by speaking, that she wishes to sign a welfare benefit form. She then enters "1-2-3-4" to identify the form she is signing. The IVR system then prompts her read 20 the signature script at the sound of the tone. Jane Doe then reads the script and it is recorded in .wav format and stored on (step 316).

25 The system then creates a process record that includes the document 304, a description of the signature process 306, and a copy the .wav file recording Jane's recitation (step 318). The signature process 306 describes how the signature program worked and how the speakable identifier was created and stored.

Years later, Sally desires to establish that Jane signed the document 304. Sally 30 engages an investigator to verify the signature. The investigator possesses only the signed document 308, which is a process record created by the signature program containing the document 302, an audio recording of Jane's assent, and a description of the signature process 304. The investigator can follow the documentation to recreate a speakable identifier from the content of the letter to establish that the audio/video recording is associated with the

document 302. The investigator can then compare the speakable identifier with the one recorded. If the two identifiers match and the voice sounds like that of Jane Doe, then the investigator possesses substantial evidence that Jane Doe did sign the letter (step 320).

Referring to FIG. 4, in another implementation, Betty Jones, a real estate broker, prepares an office lease agreement for a lessee to sign. She prepares the agreement in Adobe Portable Document Format (PDF) using a terminal 402, such as, for example, a Sony Vaio Notebook computer, running a Pentium III Intel processor, 256 megabytes of RAM, Windows XP operating system and Adobe Acrobat 5.0 software.

Jones' computer is equipped with a modem or other device that enables her to dial into an Internet service provider and connect to a Web server 404 across the Internet 406. Using Microsoft Internet Explorer 6.0 software, she accesses the Web server 404 running software (the "voice signature program") that allows her to post the lease agreement on a web page so that it may be associated with one or more voice signature messages delivered via telephone (step 414). Jones may keep a copy of the lease agreement in PDF on the hard drive of her computer.

The voice signature software is launched to begin the signatory process by assigning an identifier, such as, for example, transaction number 98765, to the lease agreement and making it available at the URL <http://www.voicesignature.com/98765> (step 416). Any World Wide Web user accessing that URL is delivered the content of the lease agreement in PDF. In addition, the voice signature software runs a digesting algorithm against all the bits that constitute the lease agreement's content, which results in a speakable electronic document identifier, "ZYXWV". This is a document identifier, as explained in U.S. Application Serial No. 10/214,444.

The voice signature software enables Jones to prepare instructions for Sam White (Jones's client) to sign the lease agreement (step 418). The instructions state that White may sign the form by calling an interactive voice response (IVR) system, indicating that he wishes to sign transaction number 98765, and speaking the following script when prompted to do so: "I Sam White hereby sign the office lease agreement. The signature code is ZYXWV."

Jones telephones White and informs him he may view the lease agreement at <http://www.voicesignature.com/98765> and that he may sign the agreement by calling a number, indicating that he wishes to sign transaction number 98765, and speaking the

following script when prompted to do so: "I Sam White hereby sign the office lease agreement. The signature code is ZYXWV."

White does not have easy access to a computer or the World Wide Web. But he trusts Jones. So he elects to sign the lease agreement without reviewing its contents in advance.

5 White calls the telephone number given by Jones using a touchtone telephone and follows the given instructions (step 420). Acting as an interactive voice response program, the voice signature software picks up the call and asks White to enter a transaction number through his touchtone keypad. White enters "9-8-7-6-5." Next, the voice signature software asks White to speak the script after the beep. When White hears the beep, he speaks these words through  
10 the telephone: "I Sam White hereby sign the office lease agreement. The signature code is ZYXWV."

The voice signature software records White's voice statement in .wav format and sends a .wav file of the statement via e-mail to Jones for storage (step 422). Jones now possesses evidence that White legally signed the content of the form stored in PDF on her  
15 computer.

In additional implementations, multiple natural expressions of assent are stored. For example, the system may guide the user, asking if the user desires to be legally bound to the terms of the agreement and asking if the user read and understood the agreement. The user's response to these queries also may be recorded to create a process record 210 incorporating  
20 multiple, perhaps independent, natural expressions of intent. In addition, the system may incorporate conventional signature techniques within a process record 210 to provide further evidence of a signer's intent.

A number of implementations have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and  
25 scope of the invention. Accordingly, other implementations are within the scope of the following claims.